AG

System for processing the data from a microcircuit card, card and reader for this system and method of implementation

Patent number: FR2710769
Publication date: 1995-04-07
Inventor: PHILIPPE CHARRIN
Applicant: INNOVATRON SECURITE INF (FR)
Classification:
- international: ***G06K19/073; G07F7/08; G07F7/10; G07F7/12;*** **G06K19/073; G07F7/08; G07F7/10; G07F7/12;** (IPC1-7): G06K19/073; G06K7/06
- european: G06K19/073; G07F7/08C; G07F7/08E4; G07F7/10D; G07F7/10D12
Application number: FR19930011722 19931001
Priority number(s): FR19930011722 19931001

Abstract of **FR2710769**

The card (10) comprises a memory (12) with at least: a non-modifiable area containing an identifying information item (13); a modifiable area containing the data to be processed (15); and a modifiable area containing a certificate (14) recalculated, during each transaction modifying the data, on the basis of at least one parameter internal to the card and at least one parameter outside the card. According to the invention, it moreover includes: read and/or write inhibitor means (17) operating selectively on the various areas of the memory so that the data area and the certificate area are modifiable only conditionally and so that the certificate area is unreadable from outside; and means (18) for comparing the certificate contained in the memory with a certificate calculated by a reader (20) cooperating with the card, in order to determine the conformity of the comparison made by the card and to authorise write access to the data area and to the certificate area only in the event of agreement.

EP 21360 (9)

AG

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 710 769**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **93 11722**

(51) Int Cl[6] : G 06 K 19/073, 7/06

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 01.10.93.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : 07.04.95 Bulletin 95/14.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *INNOVATRON SECURITE INFORMATIQUE Société Anonyme* — FR.

(72) **Inventeur(s)** : Charrin Philippe.

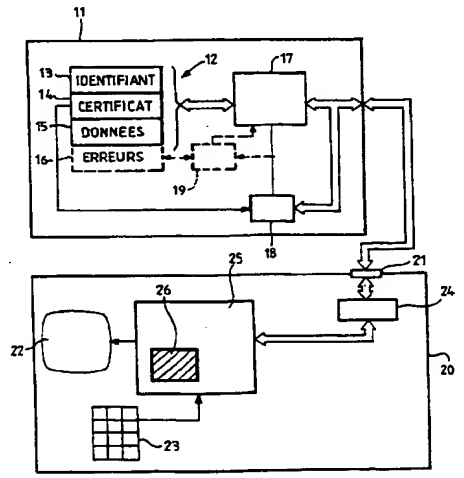
(73) **Titulaire(s)** :

(74) **Mandataire** : Dupuis-Latour Dominique, Bertrand André, Wagner Francine Avocats à la Cour.

(54) Système de traitement des données d'une carte à microcircuit, carte et lecteur pour ce système et procédé de mise en œuvre.

(57) La carte (10) comprend une mémoire (12) avec au moins: une zone non modifiable contenant une information d'identifiant (13); une zone modifiable contenant les données à traiter (15); et une zone modifiable contenant un certificat (14) recalculé, lors de chaque transaction modifiant les données, à partir d'au moins un paramètre interne à la carte et d'au moins un paramètre extérieur à la carte.

Selon l'invention, elle comporte en outre: des moyens (17) inhibiteurs de lecture et/ou d'écriture opérant sélectivement sur les différentes zones de la mémoire de manière que la zone de données et la zone de certificat ne soient modifiables que de manière conditionnelle et que la zone de certificat ne soit pas lisible de l'extérieur; et des moyens (18) pour comparer le certificat contenu dans la mémoire à un certificat calculé par un lecteur (20) coopérant avec la carte, pour déterminer la conformité de la comparaison effectuée par la carte et pour n'autoriser l'accès en écriture à la zone de données et à la zone de certificat qu'en cas de concordance.



FR 2 710 769 - A1

des informations contenues dans les zones de données) et d'une clé secrète, extérieure à la carte et propre au système, généralement non mémorisée mais recalculable par le lecteur au sein d'un « module sécuritaire », qui est un module spécial protégé à la fois physiquement et électroniquement contre les tentatives d'intrusion de fraudeurs qui voudraient tenter de retrouver la clé secrète.

Le mode de calcul de ce certificat est en lui même connu, et on ne le décrira pas plus en détail. On peut simplement indiquer qu'il a pour caractéristiques essentielles :

— d'être différent d'une carte à l'autre (en particulier parce qu'il est calculé à partir du numéro de série, qui est une information d'identification qui rend la carte unique),

— d'être différent d'une transaction à la suivante : le certificat est en effet (à la différence des codes secrets personnels du type « code porteur ») une information évolutive puisque dépendante des données, elles-mêmes évolutives, contenues dans la carte (solde comptable, nombre de transactions, etc.),

— de dépendre d'un paramètre extérieur à la carte, de sorte qu'il est impossible à un fraudeur de recalculer le certificat à partir des seules données contenues dans la carte.

Ce certificat a pour rôle de garantir l'origine des données de la carte, en permettant de certifier la provenance de celle-ci (le certificat n'ayant pu être calculé qu'à partir d'un lecteur conforme) et de n'autoriser la transaction de modification des données que si la conformité du certificat est avérée.

Le FR-A-2 653 248 décrit un tel système de traitement des données d'une carte à microcircuit faisant usage d'un certificat pour assurer la sécurité des transactions.

Néanmoins, ce système de l'art antérieur, s'il fait usage d'une carte simple et bon marché (le calcul du certificat étant effectué par le lecteur et non dans la carte), ne procure néanmoins qu'une sécurité limitée. En effet :

— en premier lieu, toutes les informations de la carte sont directement accessibles de l'extérieur, notamment l'information de certificat et les autres informations (notamment les données

nées, à partir d'au moins un paramètre interne à la carte et d'au moins un paramètre extérieur à la carte ; et au moins un lecteur comprenant : des moyens pour lire des informations dans la carte ; des moyens pour calculer un certificat à partir d'au moins certaines des informations ainsi lues et d'au moins une information contenue dans le lecteur ou déterminable par celui-ci ; et des moyens pour modifier concurremment la zone de données et la zone de certificat de la carte en cas de concordance entre le certificat calculé par le lecteur et le certificat contenu dans la carte.

Selon l'invention, ce système est caractérisé en ce que : la carte comprend des moyens inhibiteurs de lecture et/ou d'écriture opérant sélectivement sur les différentes zones de la mémoire de manière que la zone de données et la zone de certificat ne soient modifiables que de manière conditionnelle et que la zone de certificat ne soit pas lisible de l'extérieur ; la carte comprend des moyens pour comparer le certificat contenu dans la mémoire au certificat calculé par le lecteur et pour n'autoriser l'accès en écriture à la zone de données et à la zone de certificat qu'en cas de concordance ; et le lecteur comprend en outre : des moyens pour transmettre à la carte un premier certificat calculé pour comparaison par le circuit comparateur de celle-ci ; des moyens pour déterminer la conformité de la comparaison effectuée par la carte ; et des moyens pour transmettre à la carte un second certificat calculé en cas de comparaison conforme.

Très avantageusement, la mémoire comprend en outre une zone modifiable de comptage du nombre de comparaisons négatives et la carte comprend en outre des moyens pour incrémenter cette zone à chaque présentation d'un certificat non conforme et des moyens pour verrouiller la carte lorsque ce nombre atteint un seuil prédéterminé.

En ce qui concerne la détermination de la conformité de la comparaison, celle-ci peut avoir lieu notamment en effectuant les opérations d'écriture devant modifier le contenu de la zone de données après transmission à la carte du premier certificat et comparaison, et en effectuant ensuite une lecture du contenu de la zone de données et un test de vérification d'écriture. L'écriture correcte des nouvelles données implique une comparaison conforme.

notamment comporter une étape de lecture du contenu de la zone de comptage avant et après transmission à la carte du premier certificat et comparaison.

Dans une variante de mise en oeuvre, où la détermination de la conformité de la comparaison se fait en tentant d'écrire dans la zone de données et en détectant si une écriture est intervenue ou non, le procédé comporte les étapes successives consistant à : (a) lire des informations dans la carte au moyen d'un lecteur coopérant avec celle-ci ; (b) calculer par le lecteur un premier certificat à partir d'au moins certaines des informations ainsi lues et d'au moins une information contenue dans le lecteur ou déterminable par celui-ci ; (c) transmettre à la carte ce premier certificat calculé ; (d) comparer, à l'intérieur de la carte, le certificat contenu dans la mémoire de la carte à ce premier certificat calculé ; (e) tenter de modifier la zone de données, cette modification n'étant effective qu'en cas de concordance entre le premier certificat calculé et le certificat contenu dans la carte ; (f) détecter si cette modification éventuelle de la zone de données est intervenue ou non ; et (g) dans l'affirmative, transmettre à la carte un second certificat calculé par le lecteur et l'inscrire dans la zone de certificat de la carte.

◊

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description détaillée ci-dessous d'un exemple de réalisation, faite en référence aux dessins annexés.

La figure 1 est une vue schématique montrant une carte et le lecteur avec lequel elle coopère.

La figure 2 est un diagramme par blocs des organes essentiels de la carte et du lecteur servant à expliquer le fonctionnement de ces deux éléments et la manière dont ils interagissent.

◊

Sur la figure 1, la référence 10 désigne une carte portant un mi-

— avantageusement, mais non nécessairement, une zone 16 de comptage du nombre d'erreurs de présentation du certificat.

D'autres informations peuvent également être mémorisées dans la carte, par exemple un code secret de porteur (quoique l'invention soit plus particulièrement appropriée au cas des cartes anonymes, non nominatives), une zone de « signature » du lecteur ayant effectué la dernière transaction en date, etc.

La carte peut également contenir, de manière en elle-même connue, des informations qui ne sont normalement pas à la disposition des utilisateurs habituels, telles qu'une clé d'effacement permettant de réinitialiser les cartes en fin d'utilisation, par exemple lorsque les droits attachés à la carte sont épuisés (cas d'une carte porte-jetons ou porte-monnaie électronique) ou atteints (cas d'une carte pour couponnage), ou que les capacités logiques ou physiques de la mémoire de la carte sont atteintes.

Le microcircuit comporte en outre des moyens, schématisés par le bloc 17, pour contrôler sélectivement l'accès aux diverses zones de la mémoire. Ainsi :

— la zone 13 contenant l'identifiant, une fois écrite en usine, n'est plus modifiable ; elle est cependant librement lisible de l'extérieur (on notera incidemment que ce résultat peut être atteint en prévoyant des zones mémoire de natures différentes, par exemple une zone 13 en ROM ou PROM, les autres étant de type EPROM ou E^2PROM),

— la zone 14 contenant le certificat n'est jamais lisible de l'extérieur et n'est inscriptible que de façon conditionnelle (on verra par la suite de quelle manière),

— la zone 15 contenant les données est librement lisible de l'extérieur mais, de la même manière, n'est inscriptible que de façon conditionnelle,

— la zone 16 contenant le compte des erreurs n'est pas inscriptible de l'extérieur, et est gérée de façon purement interne à la carte en ce qui concerne son écriture.

Les moyens permettant de mettre en oeuvre cette inhibition sélective de lecture et/ou écriture des différentes zones mémoire sont

circuit permettant d'appliquer à cette dernière les tensions d'alimentation appropriées et les signaux et protocoles d'échange d'informations normalisé en fonction des actions souhaitées. Cette interface 24 permet à un circuit principal 25 du lecteur de communiquer avec la carte, en recevant des informations de celle-ci et en lui envoyant des informations. Ce circuit 25 comporte notamment un « circuit sécuritaire » 26, protégé physiquement et électroniquement contre les tentatives d'intrusion des fraudeurs et permettant d'effectuer le calcul d'un certificat à partir d'informations lues dans la carte (essentiellement l'identifiant de la zone 13 et les données de la zone 15) et d'une clé secrète, propre au système, recalculable de façon interne par ce même circuit 26.

On va maintenant exposer le déroulement d'une transaction opérée avec le système de l'invention.

Essentiellement, on peut envisager deux types de transactions : des transactions de lecture simple et des transactions de modification des données de la carte.

Les premières s'effectuent par simple lecture de la zone de données 15 qui est, comme on l'a expliqué plus haut, librement accessible en lecture. Les informations, par exemple le solde résiduel de la carte ou le nombre de points acquis, etc. sont affichées sur l'écran 22 du lecteur.

Les transactions de modification des données, en revanche, s'effectuent suivant une séquence particulière destinée à mettre en oeuvre l'ensemble des mesures de sécurisation nécessitées par une telle transaction.

En premier lieu, le lecteur lit dans la carte la zone 13 d'identifiant et la zone 15 de données (qui sont librement accessibles en lecture).

Les informations lues sont transférées dans le composant sécuritaire 26, qui calcule une valeur de certificat à l'aide d'un algorithme utilisant un secret détenu communément par tous les lecteurs du système et à partir de l'identifiant et des données lues dans la carte.

Le certificat ainsi calculé est alors envoyé vers la carte pour présentation au comparateur 18, qui confronte la valeur recalculée par

non conforme" en direction du lecteur, comme on pourrait l'envisager avec une carte à microprocesseur.

On peut néanmoins déduire indirectement le résultat de la comparaison en tentant tout d'abord d'inscrire les données dans la carte et en déterminant, par un test approprié, si l'écriture est effectivement intervenue.

On peut à cet effet relire la zone de données 15 et la comparer avec sa valeur antérieure, mémorisée. Si les deux contenus, avant et après la tentative d'écriture, sont les mêmes, c'est que l'écriture a été refusée par la carte et donc que la comparaison n'a pas été conforme ; l'émission vers la carte du nouveau certificat est alors refusée par le lecteur et il est mis fin à la transaction. Si en revanche la comparaison a été conforme, l'étape d'écriture est parachevée par émission du nouveau certificat vers la carte et mise à jour de la zone correspondante 14.

Une autre technique consiste à lire la valeur du compteur d'erreurs (que l'on suppose alors librement lisible de l'extérieur) avant et après la tentative d'écriture ; si la valeur du compteur a évolué, c'est que la comparaison n'a pas été conforme.

On peut voir que le système de l'invention assure une sécurité renforcée à plusieurs niveaux.

En premier lieu, du fait que la zone 14 de certificat n'est pas lisible de l'extérieur, il devient impossible de dupliquer à l'identique les cartes (ce qui constituait un risque sérieux de fraude dans le cas des cartes non nominative de l'art antérieur).

En second lieu, l'accès en écriture aux données de la carte est protégé sans pour autant qu'il soit nécessaire de confier un code d'accès au porteur — ce qui permet d'appliquer le système à des cartes non nominatives. On notera en outre que l'opérateur du lecteur ne détient non plus aucun code d'accès et que, en outre, le code d'accès utilisé (le certificat) est dynamique (il est modifié à chaque transaction et est caractéristique à la fois de la carte et de la transaction), ce qui le rend particulièrement difficile à retrouver, à la différence d'un code d'accès intangible.

En troisième lieu, le code d'accès (le certificat) n'est pas lisible de

REVENDICATIONS

1. Un système de traitement de données, comportant :

— au moins une carte (10) ou autre objet portatif à microcircuit comprenant une mémoire électronique (12) avec au moins :

- une zone non modifiable contenant une information d'identifiant spécifique de la carte (13),
- une zone modifiable contenant les données à traiter (15), notamment des données comptables à incrémenter et/ou décrémenter, et
- une zone modifiable contenant un certificat (14), ce certificat étant une valeur recalculée, lors de chaque transaction modifiant lesdites données, à partir d'au moins un paramètre interne à la carte et d'au moins un paramètre extérieur à la carte, et

— au moins un lecteur (20) comprenant : des moyens pour lire des informations dans la carte ; des moyens pour calculer un certificat à partir d'au moins certaines des informations ainsi lues et d'au moins une information contenue dans le lecteur ou déterminable par celui-ci ; et des moyens pour modifier concurremment la zone de données et la zone de certificat de la carte en cas de concordance entre le certificat calculé par le lecteur et le certificat contenu dans la carte,

système caractérisé en ce que :

— la carte comprend des moyens (17) inhibiteurs de lecture et/ou d'écriture opérant sélectivement sur les différentes zones de la mémoire de manière que la zone de données et la zone de certificat ne soient modifiables que de manière conditionnelle et que la zone de certificat ne soit pas lisible de l'extérieur,

— la carte comprend des moyens (18) pour comparer le certificat contenu dans la mémoire au certificat calculé par le lecteur et pour n'autoriser l'accès en écriture à la zone de données et à la zone de certificat qu'en cas de concordance, et

— le lecteur comprend en outre : des moyens pour transmettre à la carte un premier certificat calculé pour comparaison par le

4. Un lecteur (20) pour le système de la revendication 1, comprenant : des moyens pour lire des informations dans une carte (10) avec laquelle il coopère ; des moyens pour calculer un certificat à partir d'au moins certaines des informations ainsi lues et d'au moins une information contenue dans le lecteur ou déterminable par celui-ci ; et des moyens pour modifier concurremment une zone de données (15) et une zone de certificat (14) de la carte en cas de concordance entre le certificat calculé par le lecteur et le certificat contenu dans la carte,

lecteur caractérisé en ce qu'il comprend en outre : des moyens pour transmettre à la carte un premier certificat calculé pour comparaison par un circuit comparateur de celle-ci ; des moyens pour déterminer la conformité de la comparaison effectuée par la carte ; et des moyens pour transmettre à la carte un second certificat calculé en cas de comparaison conforme.

5. Le lecteur de la revendication 4, dans lequel les moyens pour déterminer la conformité de la comparaison effectuée par la carte comportent des moyens d'écriture et des moyens pour vérifier que l'écriture a été effectuée correctement.

6. Le lecteur de la revendication 4, dans lequel, lorsque la carte comprend une zone de comptage du nombre de comparaisons négatives, les moyens pour déterminer la conformité de la comparaison effectuée par la carte comportent des moyens pour lire le contenu de cette zone de comptage avant et après transmission à la carte du premier certificat et comparaison.

7. Un procédé de traitement des données contenues dans une carte (10) ou autre objet portatif à microcircuit comprenant une mémoire électronique avec au moins : une zone non modifiable contenant une information d'identifiant spécifique de la carte ; une zone modifiable contenant les données à traiter, notamment des données comptables à incrémenter et/ou décrémenter ; et une zone modifia-

comptables à incrémenter et/ou décrémenter ; et une zone modifiable contenant un certificat, ce certificat étant une valeur recalculée, lors de chaque transaction modifiant lesdites données, à partir d'au moins un paramètre interne à la carte et d'au moins un paramètre extérieur à la carte,

procédé caractérisé par les étapes successives consistant à :

(a) lire des informations dans la carte au moyen d'un lecteur (20) coopérant avec celle-ci ;

(b) calculer par le lecteur un premier certificat à partir d'au moins certaines des informations ainsi lues et d'au moins une information contenue dans le lecteur ou déterminable par celui-ci ;

(c) transmettre à la carte ce premier certificat calculé ;

(d) comparer, à l'intérieur de la carte, le certificat contenu dans la mémoire de la carte à ce premier certificat calculé ;

(e) tenter de modifier la zone de données, cette modification n'étant effective qu'en cas de concordance entre le premier certificat calculé et le certificat contenu dans la carte ;

(f) détecter si cette modification éventuelle de la zone de données est intervenue ou non ; et

(g) dans l'affirmative, transmettre à la carte un second certificat calculé par le lecteur et l'inscrire dans la zone de certificat de la carte.

10. Le procédé de la revendication 9, dans lequel, la carte comprenant une zone de comptage du nombre de comparaisons négatives, l'étape de détection de la modification de la zone de données comprend une lecture du contenu de cette zone de comptage avant et après transmission à la carte du premier certificat et comparaison.

REPUBLIQUE FRANÇAISE

2710769

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 492170
FR 9311722

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
D,X	FR-A-2 653 248 (GEMPLUS CARD INTERNATIONAL) * page 4, ligne 9 - page 5, ligne 6 * * page 5, ligne 34 - page 7, ligne 17 * * page 8, ligne 3 - page 9, ligne 12; figures 1,2 *	1,2,4,7,9
Y	DE-A-41 19 924 (SIEMENS AG) * colonne 2, ligne 54 - colonne 3, ligne 39; revendication 1 *	1,2,4,7,9
Y	EP-A-0 378 454 (GEMPLUS CARD INTERNATIONAL) * colonne 3, ligne 49 - colonne 4, ligne 22; revendication 1; figure *	1,2,4,7,9
A	FR-A-2 685 520 (MONETEL (SA)) * page 1, ligne 25 - page 4, ligne 11; figures 2,3 *	1,2,4,7,9
A	EP-A-0 299 826 (SCHLUMBERGER INDUSTRIES) * revendication 1; figures 1-3 *	1,2,4,7,9

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.5)

G07F

1

Date d'achèvement de la recherche	Examinateur
10 Juin 1994	Ducreau, F

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)